a) Kako je NZD(4, 9) = 1, $([4]_9)^{-1}$ postoji i njegovo računanje svodi se na nalaženje najmanjeg pozitivnog rješenja za x Diofantove jednačine $4x + 9k = 1$. Kako nam je potrebno samo rješenje za x, najpraktičnije je za nalaženje rješenja upotrijebiti Euklidov algoritam. Imamo:

$$9 = 2 \cdot 4 + 1 \Rightarrow 1 = 9 - 2 \cdot 4$$

Dakle, već u prvom koraku odmah dobijamo rastavu NZD(4, 9) = $1 = -2 \cdot 4 + 1 \cdot 9$. Stoga je opće rješenje za x datko kao $x = -2 \cdot 1 + 9t$, odnosno $x = -2 + 9t$, gdje je t proizvoljan cijeli broj. Sada, najmanje pozitivno rješenje za x dobija se za $t = 1$ i iznosi $x = 7$, pa je $([4]_9)^{-1} = [7]_9$.

Alternativno, $([4]_9)^{-1}$ možemo izračunati i pomoću modularnog stepenovanja koristeći činjenicu da je $([a]_m)^{-1} = ([a]_m)^{\varphi(m)-1}$. Kako je $\varphi(9) = \varphi(3^2) = 3^2 - 3^1 = 6$, to je $([4]_9)^{-1} = ([4]_9)^5$. Imamo

$$([4]_9)^2 = [16]_9 = [\mathrm{mod}(16, 9)]_9 = [7]_9$$
$$([4]_9)^4 = ([7]_9)^2 = [49]_9 = [\mathrm{mod}(49, 9)]_9 = [4]_9$$
$$([4]_9)^5 = ([4]_9)^4 ([4]_9) = ([4]_9)([4]_9) = [16]_9 = [\mathrm{mod}(16, 9)]_9 = [7]_9$$

Dakle, ponovo dobijamo $([4]_9)^{-1} = [7]_9$.

b) Ponovo imamo NZD(7, 17) = 1, te $([7]_{17})^{-1}$ postoji i njegovo računanje svodi se na rješavanje Diofantove jednačinu $7x + 17k = 1$. Primijenimo Euklidov algoritam:

$$17 = 2 \cdot 7 + 3 \Rightarrow 3 = 17 - 2 \cdot 7$$
$$7 = 2 \cdot 3 + 1 \Rightarrow 1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (17 - 2 \cdot 7) = 5 \cdot 7 - 2 \cdot 17$$

Slijedi da je opće rješenje za x dato kao $x = 5 + 17t$, uz proizvoljno $t \in \mathbb{Z}$. Najmanje pozitivno rješenje dobija se za $t = 0$ i iznosi $x = 5$, pa je $([7]_{17})^{-1} = [5]_{17}$.

Alternativno, kako je 17 prost broj, imamo $\varphi(17) = 17 - 1 = 16$, tako da je $([7]_{17})^{-1} = ([7]_{17})^{15}$. Primjenom algoritma "kvadriraj-i-množi" imamo:

$$([7]_{17})^2 = [49]_{17} = [\mathrm{mod}(49, 17)]_{17} = [15]_{17}$$
$$([7]_{17})^4 = ([15]_{17})^2 = [225]_{17} = [\mathrm{mod}(225, 17)]_{17} = [4]_{17}$$
$$([7]_{17})^8 = ([4]_{17})^2 = [16]_{17}$$
$$([7]_{17})^{15} = ([7]_{17})^8 ([7]_{17})^4 ([7]_{17})^2 ([7]_{17}) = ([16]_{17})([4]_{17})([15]_{17})([7]_{17}) =$$
$$= [6720]_{17} = [\mathrm{mod}(6720, 17)]_{17} = [5]_9$$

Ovim smo na drugi način potvrdili da je $([7]_{17})^{-1} = [5]_{17}$.

c) Ovdje također imamo NZD(21, 143) = 1 te $([21]_{143})^{-1}$ postoji i njegovo računanje svodi se na rješavanje Diofantove jednačine $21x + 143k = 1$, pri čemu je opet NZD(21, 143) = 1. Primijenom Euklidovog algoritma, imamo:

$$143 = 6 \cdot 21 + 17 \Rightarrow 17 = 143 - 6 \cdot 21$$
$$21 = 1 \cdot 17 + 4 \Rightarrow 4 = 21 - 17 = 21 - (143 - 6 \cdot 21) = 7 \cdot 21 - 143$$
$$17 = 4 \cdot 4 + 1 \Rightarrow 1 = 17 - 4 \cdot 4 = (143 - 6 \cdot 21) - 4 \cdot (7 \cdot 21 - 143) = -34 \cdot 21 + 5 \cdot 143$$

Odavde vidimo da opće rješenje za x glasi $x = -34 + 143t$, uz proizvoljno $t \in \mathbb{Z}$. Najmanje pozitivno rješenje dobija se za $t = 1$ i iznosi $x = 109$, pa je $([21]_{143})^{-1} = [109]_{143}$.

Izvedimo isto rješenje i pomoću modularnog stepenovanja. Kako je $143 = 11 \cdot 13$, to imamo da je $\varphi(143) = \varphi(11)\varphi(13) = (11 - 1)(13 - 1) = 120$, tako da je $([21]_{143})^{-1} = ([21]_{143})^{119}$. Dalje imamo:

$$([21]_{143})^2 = [441]_{143} = [\mathrm{mod}(441, 143)]_{143} = [12]_{143}$$
$$([21]_{143})^4 = ([12]_{143})^2 = [144]_{143} = [\mathrm{mod}(144, 143)]_{143} = [1]_{143}$$

Zbog činjenice da je $([21]_{143})^4 = [1]_{143}$ odmah slijedi i

$$([21]_{143})^8 = ([21]_{143})^{16} = ([21]_{143})^{32} = ([21]_{143})^{64} = [1]_{143}$$

Kako je $119 = 64 + 32 + 16 + 4 + 2 + 1$, to je konačno

$$\begin{aligned}([21]_{143})^{119} &= ([21]_{143})^{64}([21]_{143})^{32}([21]_{143})^{16}([21]_{143})^4([21]_{143})^2([21]_{143}) = \\ &= ([1]_{143})([1]_{143})([1]_{143})([1]_{143})([12]_{143})([21]_{143}) = [252]_{143} = \\ &= [\mathrm{mod}(252, 143)]_{143} = [109]_{143}\end{aligned}$$

Ovim je potvrđen rezultat $([21]_{143})^{-1} = [109]_{143}$. Usput, iz izloženog se vidi da je formula po kojoj je $([a]_m)^{-1} = ([a]_m)^{\varphi(m)-1}$ više od teoretskog interesa nego što predstavlja praktičan način za računanje $([a]_m)^{-1}$.

d) Kako je $\mathrm{NZD}(11, 20) = 1$, $([11]_{20})^{-1}$ postoji i njegovo raćunanje svodi se na rješavanje Diofantove jednačine $11x + 20k = 1$. Ponovo ćemo primijeniti Euklidov algoritam:

$$20 = 1 \cdot 11 + 9 \;\Rightarrow\; 9 = 20 - 11$$
$$11 = 1 \cdot 9 + 2 \;\Rightarrow\; 2 = 11 - 9 = 11 - (20 - 11) = 2 \cdot 11 - 1 \cdot 20$$
$$9 = 4 \cdot 2 + 1 \;\Rightarrow\; 1 = 9 - 4 \cdot 2 = (20 - 11) - 4 \cdot (2 \cdot 11 - 1 \cdot 20) = -9 \cdot 11 + 5 \cdot 20$$

Opće rješenje za x dato je kao $x = -9 + 20t$, uz proizvoljno $t \in \mathbb{Z}$. Najmanje pozitivno rješenje dobija se za $t = 1$ i iznosi $x = 11$, pa je $([11]_{20})^{-1} = [11]_{20}$, odnosno element $[11]_{20}$ je sam sebi inverzan.

Interesantno je i provjeriti ovo rješenje pomoću modularnog stepenovanja. Kako je $20 = 2^2 \cdot 5$, to je $\varphi(20) = \varphi(2^2)\varphi(5) = (2^2 - 2^1)(5 - 1) = 8$, tako da je $([11]_{20})^{-1} = ([11]_{20})^7$. Sada je:

$$([11]_{20})^2 = [121]_{20} = [\mathrm{mod}(121, 20)]_{143} = [1]_{20}$$
$$([11]_{20})^4 = ([1]_{20})^2 = [1]_{20}$$
$$([11]_{20})^7 = ([1]_{20})^4([1]_{20})^2([1]_{20}) = ([1]_{20})([1]_{20})([11]_{20}) = [11]_{20}$$

Dakle, zaista je $([11]_{20})^{-1} = [11]_{20}$. Ovo je zapravo posljedica činjenice da je $([11]_{20^{-1}})^2 = [1]_{20}$. Inače, za elemente $[a]_m$ za koje je $([a]_m)^2 = [1]_m$ kaže se da su *idempotentni*. Iz same definicije inverznih elemenata slijedi da su idempotentni elementi ujedno i sami sebi inverzni, tj. da za njih vrijedi $([a]_m)^{-1} = [a]_m$.

e) Kako je $\mathrm{NZD}(35, 210) = 35$, to $([35]_{210})^{-1}$ ne postoji, odnosno element $[35]_{210}$ nije invertibilan. Zaista, računanje $([35]_{210})^{-1}$ svodilo bi se na rješavanje Diofantove jednačine $35x + 210k = 1$ koja nije rješiva.